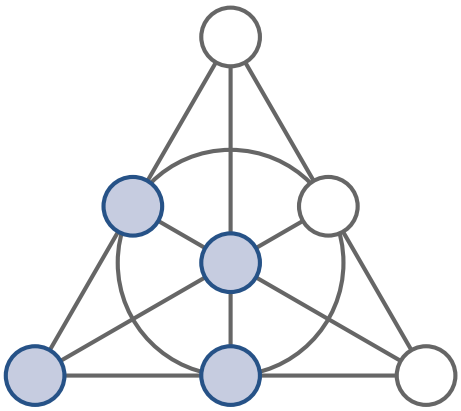
o-Polynomials and Explicit Formula for o-Monomials

Ursprünglich wurden projektive Geometrien entwickelt um Zeichnungen in Perspektive zu ermöglichen. Heute gibt es zu ihnen eine sehr reichhaltige Theorie, insbesondere lassen sich auch über endlichen Körpern projektive Geometrien definieren. In diesen sogenannten endlichen Desarguesschen Geometrien sind kombinatorisch (und auch in Anwendungen in der Codierungstheorie) besonders Bögen interessant: Das sind Mengen von Punkten der Geometrie, von denen je drei nicht auf einer gemeinsamen Gerade liegen. In dieser Arbeit wurde die Situation der Bögen mit maximal vielen Punkten in den projektiven Ebenen betrachtet.

Wenn die Charakteristik des zugrundeliegenden Körpers ungerade ist, spricht man von Ovalen und bei gerader Charakteristik von Hyperovalen. Obwohl bereits 1955 von Segre gezeigt wurde, dass Ovale nichtsinguläre Kegelschnitte sind und damit sehr gut verstanden sind, verhalten sich Hyperovale ganz anders und werfen auch weiterhin viele Fragen auf. Sie sind größer und ihre Klassifikation bleibt ein wichtiges Problem. In der Abbildung ist in blau ein Hyperoval in der sogenannten Fano-Ebene abgebildet.



Ein wichtiger Aspekt von Hyperovalen ist die Assoziation mit sogenannten o-Polynomen über binären endlichen Körpern, die eine algebraische Darstellung und Untersuchung dieser Objekte ermöglicht. In der Arbeit wird zuerst diese spannende Theorie erläutert. Insbesondere wird dabei eine Äquivalenzrelation untersucht, aus der sich Transformationen gewinnen lassen, durch die ein gegebenes o-Polynom in ein neues überführt werden kann. Für die bekannten o-Monome werden dann alle solchen Transformierten explizit berechnet.

Nützlich für eine konkrete Anwendung von o-Polynomen ist ihre enge Verbindung zu 2-zu-1 Polynomen, die sich aus der Bogeneigenschaft ergibt. Gerade die o-Monome führen dann zu 2-zu-1 Binomen, die in der Kryptografie und Theorie der endlichen Körper aktuell untersucht werden. Über die vorher berechneten Formeln lassen sich so einige 2-zu-1 Binome konstruieren.

Da die Bogeneigenschaft natürlich auch für Ovale in ungerader Charakteristik gilt, lassen sich die Verbindungen zu den 2-zu-1 Polynomen auch in diesem bisher unerforschten Fall untersuchen und ausnutzen. Da die Ovale aber sehr gut verstanden sind, konnte so für einen Typ von 2-zu-1 Binomen in dieser Arbeit eine Klassifizierung erzielt werden.